(12) UK Patent Application (19) GB (11) 2 389 928 (13) A

(43) Date of A Publication 24.12.2003

(21) Application No: 0214407.9

(22) Date of Filing: 21.06.2002

(71) Applicant(s):
Spero Communications Limited
(Incorporated in the United Kingdom)
Meridian Gate, Marsh Wall,
London Docklands, LONDON, E14 9YT,
United Kingdom

(72) Inventor(s):
Ian Douglas Spero

(74) Agent and/or Address for Service:
Boult Wade Tennant
Verulam Gardens, 70 Gray's Inn Road,
LONDON, WC1X 8BT, United Kingdom

(51) INT CL[7]:
G06F 1/00

(52) UK CL (Edition V):
G4A AAP A23A A23E

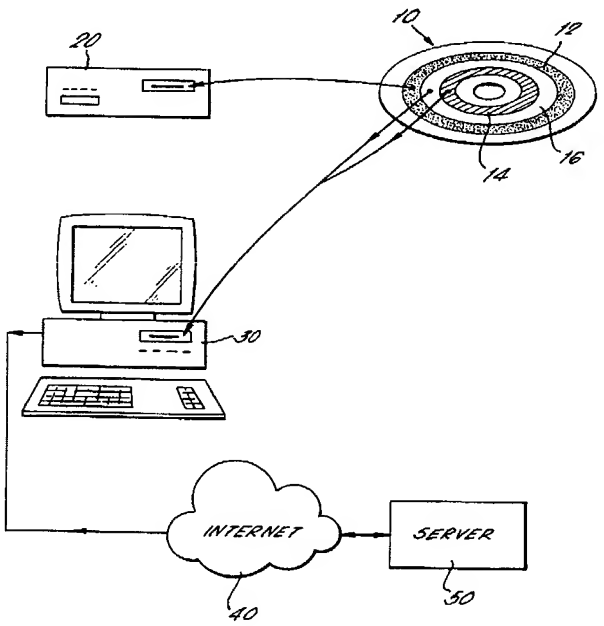
(56) Documents Cited:
EP 1077398 A1
WO 2001/090860 A2
US 5991402 B
US 5416840 B
WO 2003/010637 A1
WO 1996/041445 A1
US 5903650 B

(58) Field of Search:
INT CL[7] **G06F**
Other: **Online: WPI, EPODOC, JAPIO**

(54) Abstract Title: **Data stored in encrypted form on a data carrier may be accessed by a user when a remote server provides permission**

(57) A user who wishes to access encrypted data stored on a data carrier, such as a CD or DVD 10, must contact a sewer 50 to request access to the data. If the user is entitled to access the data the sewer will return a decryption key to the user's computer 30 to allow the user to decrypt the data. When the user issues the request to the sewer he may provide registration or/and payment data. The data carrier may also contain unencrypted data such as demonstration audio tracks or video data, allowing the user to try some of the information on the data carrier before paying for access to encrypted content. Preferably the user may access the trial data using standard playback apparatus 20 which has no decryption capability. The data carrier may also contain control data which limits use of the encrypted data to a predetermined number of uses, or a predetermined period of time. There may also be provided means to allow the user to order an additional product related to the encrypted data.

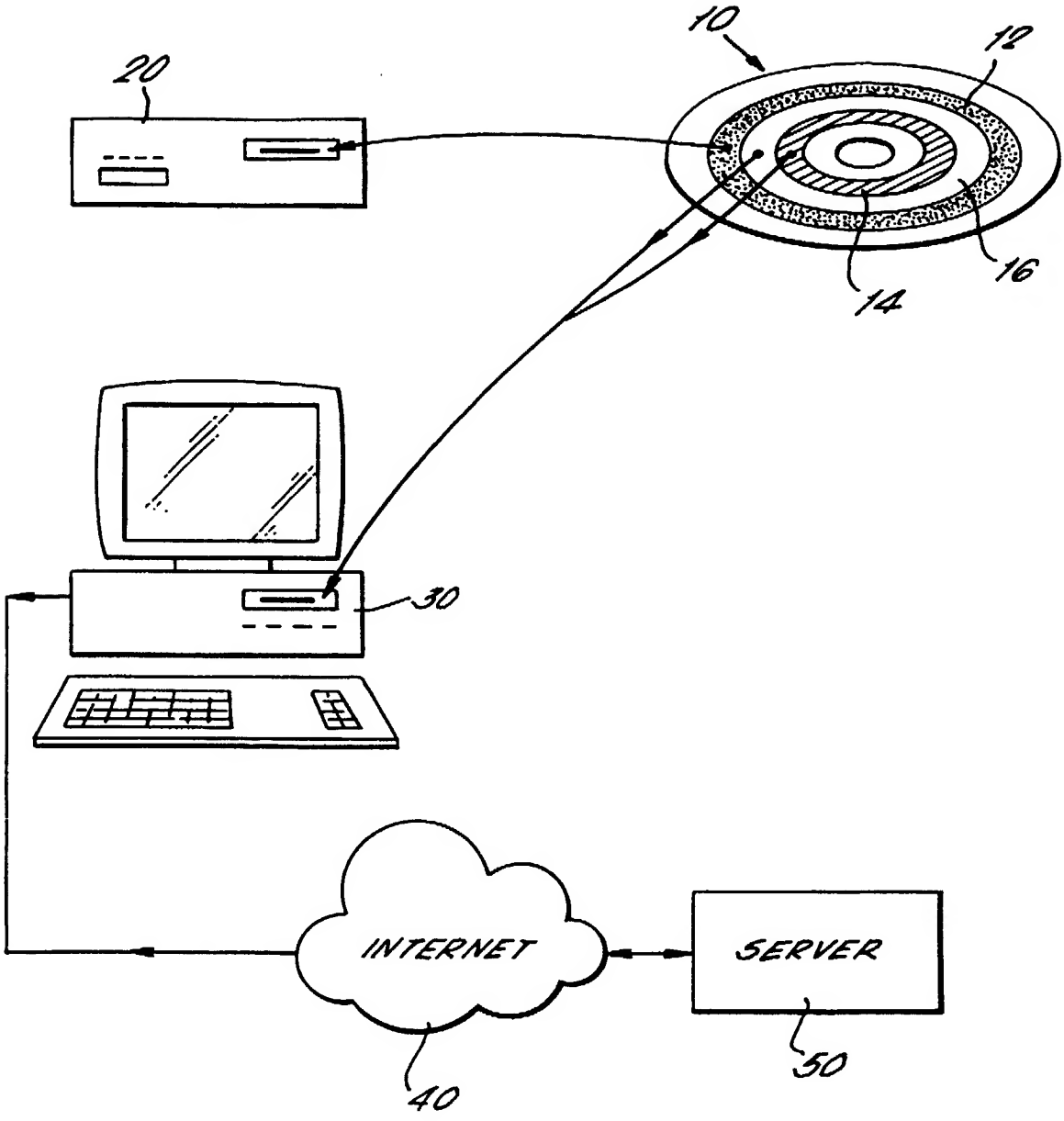
FIG. 1.



GB 2 389 928 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

FIG. 1.



2389928

ENABLING USE OF ENCRYPTED DATA

The present invention relates to method of enabling use or playback of encrypted data, to a medium carrying encrypted data and to associated playback apparatus. In particular, but not exclusively, the invention relates to encrypted audio and/or video data carried on an optical disk such as a Compact Disk or Digital Versatile Disk.

Much effort has been expended in recent years in seeking techniques for effective commercial distribution of valuable electronic data by telecommunications means, such as over the Internet or cell phone networks, rather than by more traditional physical means including analogue audio tapes, records and Compact Disks. A principal problem with such telecommunications distribution is the ease with which the delivered electronic data can be subsequently copied and the associated rights abused, usually by breach of copyright and the contract between the supplier and consumer. Data rights management systems such as the Electronic Media Management System (EMMS) developed by IBM encrypt electronic data, and in particular audio and video data. By controlling the decryption process, such systems seek to control the extent to which a consumer can replay and make further copies of the electronic data.

Despite the recent dramatic rise in the use of telecommunications for retail and data distribution purposes, physical media such as Compact Disks remain by far the most commercially important retail mechanism for audio and video products. In consequence, conventional domestic playback devices such as standalone CD and DVD players remain much more popular than, for example, appropriately programmed personal computers for playback of audio and video products.

The present invention provides a method of enabling playback of encrypted audio and/or video and/or other data by a client computer system, comprising the steps of providing a data carrying medium comprising said encrypted data for access by said client computer system; receiving request data at a server computer system, over a network from said client computer system; in response to receiving said request data, transmitting permission data from said server computer system over said network to said client computer system, said permission data being arranged to enable decryption and use or playback of said data by said client computer system.

Preferably, the data carrying medium is an optical disk such as a Compact Disk or Digital Versatile Disk.

Preferably, unencrypted audio and/or video, and/or other data is also written on the data carrying medium, for example audio and/or video data for playback using a conventional domestic CD or DVD player.

Preferably, the permission data transmitted from the server computer to the client computer contains decryption key data required to carry out decryption of the encrypted data by the client computer system.

Preferably, the data carrying medium comprises data which restricts the decryption and/or playback or other use of the encrypted data. For example, the number of times which the data may be played or used, or a time period within which it may be played or used may be restricted.

Preferably, the data carrying medium also comprises computer software code which, when executed on the client computer system, is adapted to carry out or enable the decryption and use/playback processes. The decryption may be reliant on a decryption key or keys received from the server computer system.

Preferably, this computer software code is also adapted to direct the transmission of the request data to the server computer and to direct receipt of the permission data.

Advantageously, the computer software provided on the data carrying medium may also be operable to provide a facility for ordering, over the network, a data product such as an electronic data product or a Compact Disk or Digital Versatile Disk, and in particular such a product associated with the encrypted audio and/or visual data.

Advantageously, the client computer system may be required to provide particular items of registration data when sending the request to the server computer system for authorisation or a decryption key to decrypt and playback or use the data on the data carrying medium.

The invention also provides a data carrying medium comprising unencrypted audio and/or video or other data configured for playback or use by a conventional playback device, such as a domestic CD or DVD player, and encrypted audio and/or video or other data configured for restricted playback by a decrypting playback device, such as an appropriately programmed personal computer. Preferably, the decrypting playback device is provided through the installation on a personal computer of appropriate playback computer software code provided on the data carrying medium.

Preferably, the playback computer software code comprises program code for directing requests, across a network to a server computer, for authorisation to decrypt at least a part of said encrypted data. Such authorisation may include a decryption key, transmitted from the server to the executing playback computer software, to enable decryption of the encrypted data.

The invention also provides a method of promoting a product, and in particular an audio or video product by providing to potential customers a data medium on which a portion, or the whole of the product is written in an encrypted format. The portion or the whole of the product may, for example, be one or more music tracks from a music album. The encrypted data is only accessible to a potential customer by using appropriate hardware and/or software, for example playback software executable on a personal computer and adapted to decrypt the data. The data medium may be supplied, for example, as an attachment to or an inclusion with a publication such as a newspaper or a magazine.

Typically, the data medium may be a Compact Disk or a Digital Versatile Disk, the encrypted data comprising audio and/or video data. The playback software is configured to decrypt and enable playback of the encrypted data, but preferably only allows limited or restricted playback, for example only allowing a predetermined number of playbacks or only allowing playback prior to a predetermined date and/or time. The predetermined factors are preferably encoded on the data medium in association with the encrypted data, but could be obtained from a remote computer server system over a network or could be fixed or determined by data associated with the playback software.

Typically, the playback software is executed on a conventional personal computer having a peripheral device operable to read the data medium, and one or more peripheral devices adapted to effect the playback. The playback software may be provided on the data medium for installation on the personal computer or similar device, or may be pre-installed, or available from other sources for installation on the personal computer.

Playback may be limited, prevented or otherwise controlled on the basis of the user obtaining a key, for example a key for decrypting the encrypted data. The playback software may be operable to obtain the key from a remote server computer accessible over a network such as the Internet. Supply of the key by the server may be dependent on the user providing user data, for example by means of an electronic registration process. Such user data will typically comprise at least some of the user's name, address, age, music or video preferences and so on. Even when the key has been supplied by the server to the user's computer, access to the encrypted data may still be limited, for example to a predetermined number of playbacks.

The playback software, or associated software, may also enable or prompt the user to order an unrestricted and/or full copy of the product, for example over the Internet. This functionality may be provided as part of the playback software itself or partly or fully by way of configuration data usable by a conventional Internet browser or other software executing on the user's computer. Equally, there may be provided means enabling the user to pre-pay, for example over the Internet, for a copy of the unrestricted and/or full product, to be collected from a retail outlet.

Advantageously, the data medium may also contain unencrypted data, such as audio or video data, and in particular such data forming a portion of the relevant product, which may be played back by a conventional domestic playback device such as a conventional CD player or DVD player. In this way, a recipient of the data medium can quickly and easily gain access to a first portion of the product before deciding, or to be encouraged to use the data medium with a personal computer to gain access to further parts or the whole

of the product, at least to a limited extent.

While the invention is particularly applicable to the distribution of audio and/or video data, it may also be applied to the distribution of other data types, including, but not limited to text, images and software code, for example interactive software such as computer games.

Embodiments of the present invention will now be described, by way of example, with reference to the accompanying drawing which illustrates a data carrying medium according to the invention along with associated apparatus for its use.

Referring to the Figure, there is shown an optical disk, and in particular a Compact Disk 10. Three groups of data stored on the Compact Disk 10 are illustrated. An unencrypted soundtrack data group 12 contains audio data which can be read and played back using a conventional domestic CD or DVD player 20. This data is encoded using the standard red book encoding used for conventional audio CDs.

An encrypted soundtrack group 14 contains audio data which cannot be played back on a conventional domestic CD or DVD player 20. Instead, this encrypted soundtrack group 14 is read, decrypted and played back using appropriate software executing on a personal computer 30 equipped with a CD ROM reader and audio playback peripherals, typically comprising a sound card and loudspeakers. If the subject data is video instead of just audio data, playback requires appropriate video playback facilities, present on most personal computers.

An operational data group 16 stored on the Compact Disk 10 contains playback software for installation on the personal computer 30, for carrying out the decryption and playback functions.

The playback software allows only restricted playback of the encrypted soundtracks 14. The extent

to which playback is restricted is determined by data held on the Compact Disk 10, either in the operation data group 16, or more preferably embedded within the encrypted sound track group 14. Playback may be restricted, for example, to a predetermined number of playbacks or prior to a predetermined date and/or time. Copying of the soundtracks when decrypted is preferably prevented or protected against by the playback software executing on the personal computer 30.

Playback of the encrypted soundtracks 14 may also be restricted according to access permissions gained by communication of the personal computer 30 over a network such as the Internet 40 with a distant server computer 50. In the preferred embodiment, such access permissions take the form of a key transmitted to the personal computer 30 by the server computer 50, the key being required to effect part or all of the decryption of the encrypted soundtracks 14.

Before receiving the key the user of the personal computer 30 is required to complete a registration process, sending user data such as his name, address, age and musical preferences to the server computer 50. The registration process and process of obtaining the key may be directed, at the personal computer 30, by the playback software, or partly or wholly by other software such as a conventional Internet browser, preferably configured to carry out the relevant processes by data and/or software held on the Compact Disk 10.

In an alternative embodiment, the user gains access to encrypted soundtracks by effecting one or more financial transactions with the server computer, which provides permission data such as appropriate decryption keys for parts of the encrypted soundtrack data according to the financial transactions. The permissions accorded may or may not be time limited,

for example to extend already payed for useage time or to gain access to new material.

In the preferred embodiment the content of the unencrypted soundtrack data group 12 is not protected in any way, being set out according to the red book audio CD Standard. The encrypted sound track data group 14 contains audio tracks wrapped in the IBM EMMS Superdistribution format. The data in this group remains encrypted at all times on the personal computer 30. The EMMS tamper-resistant technology resists hack attempts to step through playback code or to use a debugger to control execution in attempts to discover decryption keys, decryption algorithms, or to obtain decrypted content from memory buffers on the personal computer 30 during playback. Audio content is kept encrypted until it is fed to the personal computer sound card for playback. Of course, it is very difficult to prevent copying of the sound card output, which is typically in an analogue form.

EMMS attempts to prohibit recording during playback when it detects recording applications running on the same computer system. Content and decryption keys stored in the end user computer system are uniquely encrypted for that system so that each end user has a different encrypted version of each audio track. In the preferred embodiment the user is restricted to only four playbacks of the encrypted audio data, or alternatively playback until a predetermined date, although a variety of other schemes and parameters could be used.

The personal computer 10 may be enabled to allow copying and sending to others, for example by e-mail, of encrypted soundtrack data from the Compact Disk 10. If recipients of such copied or e-mailed data have appropriate playback software they will also be able to play back the encrypted soundtracks subject to the predetermined playback limitations, which are stored

with the soundtrack data. The EMMS technology prevents circumvention of the playback restrictions by deleting and reloading soundtracks or by resetting the system clock to attempt to regain access to a track for which a time period has expired.

In the preferred embodiment, the playback software is a fully integrated multimedia application/player which provides embedded and dynamic access to free and DRM/EMMS protected content including music, video and metadata (e.g. text, still and animated images, computer software and so on). Quicktime video software technology is incorporated for providing video playback and Dolby and/or CODEC technology is incorporated for supporting audio playback. The Compact Disk 10 of the preferred embodiment contains rights protected and non-rights protected content and data. The online registration process is adapted to capture marketing data, and on completion releases all DRM/EMMS protected content on the Compact Disk through the download of a permission key. Internet access is facilitated through an in-built browser window in the playback software allowing a user to access the Internet from within the playback environment.

The technology described above may advantageously be used to promote a media product such as a musical album or a video DVD. Typically, an optical disk is attached to or enclosed with a publication such as a newspaper or magazine. The optical disk contains one or more soundtracks which can be played on a conventional domestic CD or DVD player to provide the consumer with a taster and to encourage them to proceed to use the disk in their personal computer. When used on the personal computer the disk may auto-install the appropriate playback software and guide the user through the registration process, in communication with a server computer over the

Internet, in order to obtain the appropriate permission(s) and/or key(s) to decrypt protected data on the disk. In this way, the user may obtain full or limited access to audio/video data on the disk in exchange for providing marketing data. The software provided on the disk may also invite the user to order the full product which is being promoted by the disk. The full product could be delivered as a conventional CD or other optical disk, or could be delivered over the Internet as an electronic product. The server computer or a related computer system may be programmed to subsequently e-mail a user who does not order the product, to provide them with a further opportunity to order, perhaps also providing electronic permissions to provide further or continued access to part or all of the encrypted data on the disk.

The technology may also be advantageously used to promote or sell a media product by providing a part of the product unencrypted and access free, and providing access to other parts of the product only on payment of a fee or fees, or an completion of a particular transaction. For example, a CD may contain a complete musical album, but only one or a few tracks are unencrypted and immediately playable, payment and obtaining one or more decryption keys being required to gain access to further tracks. Such access may be time or repeat restricted as discussed above.

CLAIMS

1. A method of enabling use of encrypted data by a client computer system, comprising the steps of:

providing a data carrying medium comprising said encrypted data for access by said client computer system;

receiving request data at a server computer system, over a network from said client computer system;

in response to receiving said request data, transmitting permission data from said server computer system over said network to said client computer system, said permission data being arranged to enable decryption and use of at least a part of said data by said client computer system.

2. The method of claim 1 further comprising the step of providing unencrypted data on said data carrying medium.

3. The method of any preceding claims wherein said permission data comprises decryption key data required to carry out decryption of said encrypted data.

4. The method of any preceding claim further comprising the step of encoding on said data carrying medium control data which restricts decryption and/or use of said encrypted data by said client computer system.

5. The method of any preceding claim further comprising the step of providing on said data carrying medium computer software code which, when executed on

said client computer system, is operable to carry out decryption and enable use of said encrypted data.

6. The method of claim 5 wherein said computer software code is further operable to direct transmission of said request data to said server computer system and to receive said permission data from said server computer system.

7. The method of either of claims 5 or 6 wherein said computer software is further operable, when executed on said client computer system, to provide a facility for ordering, over said network, a data product associated with said encrypted data.

8. The method of any preceding claim wherein said encrypted data is protected by an electronic media management system.

9. The method of any preceding claim wherein said request data includes registration data relating to the user of the client computer system.

10. The method of any of claims 1 to 9 wherein said encrypted data comprises at least one of encrypted audio and encrypted video data.

11. The method of claim 11 wherein the step of enabling use of said audio and/or video data comprises enabling playback of said data.

12. The method of any of claims 1 to 9 wherein said encrypted data comprises a software product.

13. A data carrying medium comprising:

unencrypted audio and/or video data configured for playback by a conventional playback device; and

encrypted audio and/or video data configured for restricted playback by a decrypting playback device.

14. The data carrying medium of claim 13 further comprising playback computer software code which, when installed on a suitable computer system, causes said computer system to be operable as said decrypting playback device.

15. The data carrying medium of claim 14 wherein said playback computer software code comprises program code for directing a request, across a network to a server computer, for authorisation to decrypt said encrypted audio and/or visual data.

16. The data carrying medium of claim 15 wherein said playback computer software code comprises program code for receiving, across a network from a server computer, decryption key data for decryption of said encrypted audio and/or video data, in response to said request.

17. The data carrying medium of claim 16 wherein said playback computer software code is operable to forward to said server computer registration data relating to a user of the software code in association with the request for authorisation.

18. Playback apparatus comprising:

a reading device for reading encrypted audio and/or video data from a data carrying medium;

a decryption element adapted to decrypt at least some of said encrypted audio and/or video data in accordance with permission data; and

a reproduction element adapted to play back the decrypted audio and/or video data,

the playback apparatus being adapted to transmit

request data to a server computer system, and to receive said permission data in reply.

19. The apparatus of claim 18 wherein said permission data comprises a decryption key required to decrypt at least a part of said encrypted audio and/or video data.

20. A method of promoting an audio and/or video and/or other data product comprising the step of providing a data carrying medium carrying a first part of said product in an unencrypted format and carrying a second part of said product in an encrypted format.

21. The method of claim 20 further comprising the step of providing a decryption key for decryption of said second part of said product on request as part of a transaction.

22. The method of either of claims 20 or 21 wherein said transaction comprises a registration transaction and/or a financial transaction.

23. The method of any of claims 19 to 22 further comprising the step of restricting use of said second part of said product using an electronic media management system.

24. The method of claim 19 wherein use of said second part of said product is limited to either a predetermined number of uses or to uses before a predetermined time and date, or both.

25. The method of any of claims 19 to 24 wherein the data carrying medium is one of a Compact Disk or a Digital Versatile Disk.

26. The method of any of claims 17 to 21 further comprising the step of distributing said data carrying medium to potential customers of said product.

The Patent Office

INVESTOR IN PEOPLE

Application No: GB 0214407.9 **Examiner:** John Cullen
Claims searched: 1-12, 18-26 **Date of search:** 2 October 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance	
X, Y	X: 1, 2, 4, 9, 18, 20, 22, 24 at least Y: 7	WO 1996/041445 A1	(SPYRUS) See whole document, but in particular Abstract, lines 20-25 of p5, lines 23-26 of p24 and lines 27 and 28 of p26.
X, Y	X: 1, 2, 4, 9, 18, 20, 22, 24 at least Y: 7	EP 1077398 A1	(IBM) See whole document, but in particular the Abstract and paras. 43, 115 and 116.
X, E	1, 2, 9, 18, 20, 22 at least	WO 2003/010637 A1	(JACOB) See Abstract, Figs 1 and 2a and line 6 of p12 to line 31 of p13.
X	1, 2, 4, 7, 18, 20, 24 at least	US 5991402	(AEGLSOFT) See Abstract, Fig. 2, lines 8-26 of col. 4, and line 55 of col. 5 - line 35 of col. 6
Y	7	WO 2001/090860 A2	(WIND UP) See Abstract
X, Y	X: 1, 2, 18, 20 at least Y: 7	US 5416840	(PHOENIX) See Abstract, Figs. 3 and 5B, and lines 32-35 of col. 3.
X, Y	X: 1, 2, 18, 20 at least Y: 7	US 5903650	(NOVELL) See Abstract, Fig. 5 and line 16 of col. 3 to line 18 of col. 4.

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[V]:

Application No:	GB 0214407.9	**Examiner:**	John Cullen
Claims searched:	1-12, 18-26	**Date of search:**	2 October 2003

None

Worldwide search of patent documents classified in the following areas of the IPC[7]:

G06F

The following online and other databases have been used in the preparation of this search report:

Online: WPI, EPODOC, JAPIO